1-1-2007

Security's 'will to truth' in New Zealand's regulation of electronic crime & the (in)security reflex.

Christian Pasiak
University of Windsor

SECURITY'S 'WILL TO TRUTH' IN NEW ZEALAND'S REGULATION OF ELECTRONIC CRIME & THE (IN)SECURITY REFLEX

by

Christian Pasiak

A Thesis
Submitted to the Faculty of Graduate Studies
through the Department of Sociology and Anthropology
in Partial Fulfillment of the Requirements for
the Degree of Master of Arts at the
University of Windsor

Windsor, Ontario, Canada

2007

Your file Votre référence
ISBN: 978-0-494-42240-3
Our file Notre référence
ISBN: 978-0-494-42240-3

ABSTRACT

This dissertation offers a discourse analytic approach to representations of 'security' and its performative functions through an examination of the governance of electronic crime (or 'cyber-security') in New Zealand. Drawing from Jef Huysmans and the Stockholm School's (Barry Buzan, Ole Wæver, etc.) approach to securitization, the question of 'the real' is bracketed to paint a picture of something like a semiotic regime where, following from ontological insecurity and inchoate fears about the unknown in late modernity, surveillance and monitoring are employed by government and private enterprises in information-gathering practices to categorize strangers into 'friends' and 'enemies,' danger subsequently concretized in synoptic and mediated representations of what should be of common concern. This is argued to create a perception of determinability in terms of being able to locate 'real' unknown threats, which in turn creates further ontological insecurities about not being able to deal with such politicized insecurities (in addition to the potentially limitless realm of unknown fears). This is portrayed as an '(in)security reflex,' a process that serves particular interests where 'security' utterances are employed with the goal of creating *perceptions* of merit (the participants involved in this process scarcely constructing pictures of 'real' merit, differing from crime-preventive mentalities) to enhance the perceived legitimacy of commercial and government security providers. Such enterprises are shown to thrive in realms of indeterminability, (in)security then being a particularly opportunistic enterprise as new threats could potentially be created ad infinitum.

ACKNOWLEDGEMENTS

I would like to thank my thesis committee for their input and suggestions for this project. I am particularly grateful to Dr. Willem de Lint for his mentorship and guidance during my program of study at the University of Windsor, and without whom this research would not have been possible. I am indebted to him for allowing me free reign over the interviews that are discussed here (originally compiled for another research project that had been indefinitely postponed), as well as to Katie Nimmo and Mike Lloyd at Victoria University of Wellington in New Zealand who played a vital role in conducting and transcribing the interviews prior to my involvement.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

CERT – Computer Emergency Response Team

CCIP – Centre for Critical Infrastructure Protection

E-Crime – Electronic Crime

GCSB – Government Communications Security Bureau

IP – Internet Protocol

ISP – Internet Service Provider

MED – Ministry of Economic Development

OS – Operating System

RIPA – Regulation of Investigatory Powers Act

SIS – Security Intelligence Service

Telco – Telecommunications Company

INTRODUCTION

Though 'security' is a word frequently on the lips of politicians, media spokespersons and commercial security providers who have made a business out of its utterance, it has yet to escape its self-referential paradigm in public discourse. In New Zealand, concern about the borderless nature of electronic communications and the potential for infiltration by unknown (foreign) threats has translated into legislation providing increased monitoring capabilities for government agencies, as well as the creation of the Centre for Critical Infrastructure Protection (CCIP), a 'watch and warn' service that provides information about potential threats to critical infrastructure providers. Being a site that has been blooming with new enterprises that seek to address the issue of security, this research will examine New Zealand's regulation of electronic crime in order to wade through the murky waters in which 'security' is submerged to evaluate its performative functions.

The conceptual framework and analysis offered here is extrapolated from qualitative data representing a pool of thirty semi-structured interviews that addressed a wide array of issues surrounding security and regulation of electronic networks; these often pertained to the internet, under the rubric of 'cyber-security.' Interviews were obtained through a chain-referral model, participants then representing diverse backgrounds and organisations including commercial security consultants, individuals from various departments within police services, the CCIP, the Internet Society of New Zealand, the Cyber Crime Centre, the Censorship Compliance Unit, political parties, watchdog organisations, critical infrastructure providers, independent security contractors, network engineers, systems administrators, and internet service providers (ISPs) [1].

In this paper I will draw from Jef Huysmans and follow the Stockholm school (Wæver, Buzan, etc.) in conceptualizing the regulation of electronic crime as a process of securitization (ex: 'cyber-security'). This means I will bracket the question of 'the real' and proceed by developing a diagram of the interaction between information-gathering

[1] Ethics for the interviews was cleared through the Human Ethics Committee at Victory University of Wellington, New Zealand. Interviews were conducted between January and August 2002. Interviews are referenced here as P01, P02, etc.

and monitoring, the categorization of security into politics, and the concretization of dangers that 'started' as ontological insecurity. In this regard, I acknowledge that I am choosing as a starting point some notion of the existence of real insecurities that are parlayed into discursive and politicized instruments and that my argument is prone to Andrew Neal's (2006) critique where security's exceptionalism is distinguished from the norm, and the critique that securitization already takes on too much from the classic, liberal, modernist version to remake the image of security. My response to this is that the field both of security studies and securitization is already thickly construed by each of these dimensions: classical thought, liberal categories, modernist doubt. In other words, this paper is situated more closely between the Stockholm and Parisian schools[2] of security studies and intends to elaborate the securitization process with reference to the establishment of a governance regime for electronic crime in New Zealand[3].

What follows is, firstly, a review of concepts informing the analysis of the interviews on which this research is based, emphasizing the discursive functionality of security. Secondly, it will be argued that the construction of security agendas in New Zealand, particularly with relation to 'cyber-security,' reflected an effects-based governmentality where perceived credibility overshadowed actual danger prevention; here, success was often contingent on *creating* ontological insecurity (fear of not knowing). Thirdly is an examination of new enterprises that have emerged in New Zealand to provide services or legislation to address perceived dangers. Fourthly, trust, and its relation to monitoring is discussed within the context of security, informed by monitoring practises in New Zealand. Finally, the politicization of security will be evaluated, ultimately arguing that ontological insecurities created by fabricated danger are part of a reflexive cycle that perpetuates insecurity.

SECURITY AND THE 'WILL TO TRUTH'

Jef Huysmans (1998) has suggested that the realm of 'the political' is becoming increasingly entangled with security – interpreted as a life strategy; a culturally-established practice to mediate our relation to death – in a reflexive process of

[2] For a discussion of different security 'schools' and their critical approaches to security, see C.A.S.E. (Critical Approaches to Security in Europe) COLLECTIVE, 2006.
[3] I acknowledge Willem de Lint here for providing recommendations for the thrust of this paragraph.

(re)substantiation. The wider performative functions that follow from decisively crafted security utterances are, however, often overlooked in lieu of security studies that seek to define security (condensing meaning into a statement), or offer conceptual analyses (formulating a common denominator with which to organise an explicit meaning). Huysmans argues that, though an increasing degree of sophistication follows from the former to the latter approach, neither have sufficiently dealt with the *meaning* of security – that is, the signifying work of the noun 'security' itself, and thus, further studies in this purview should seek to address security from a 'thick signifier' approach (1998:226-239).

In this vein, Huysmans draws from Michel Foucault's contributions to understanding orders of discourse, whereby he unpacks the 'will to truth' (Foucault, 1971:10) present in axiomatic understandings of security by recognizing what might be seen as a system of exclusion that creates a division governing the process of development in our 'will to knowledge' (Foucault, 1971:10). Systems of exclusion, such as those rooted in the 'will to truth,' are rendered possible through institutional support and the subsequent ways that knowledge, thus affected, finds itself proliferating in society. This "tends to exercise a sort of pressure, a power of constraint upon other forms of discourse" (Foucault, 1971:11). This perhaps deserves some clarification to avoid that which might seem inaccessibly abstruse.

Elaborating on what is meant by security as a signifier, meaning for the signifier can be seen to derive from a process of differentiation from *other* signifiers ('security' is not 'virus') in a chain of signifiers ('security is threatened by increased connectivity to the internet'). Huysmans refers to the register of meaning that is articulated in employing 'security' as a 'security formation,' which provides intelligibility – what the 'thickness' refers to. As such, 'security' is not a "neutral device," but rather, "has a history and implies a meaning, a particular signification of social relations" (1998:228). The signifier 'security' acquires a *performative* function (rather than merely being descriptive) where "'security' becomes self-referential. It does not refer to an external, objective reality but establishes a security situation in itself," its own enunciation constituting an '(in)security condition' (Huysmans, 1998:232). The usage of 'security,' then, involves a process that activates the politics of the signifier, thus ordering social relations. A research agenda that follows from an examination of the thick signifier then "explores this register of

meaning and differences or changes in the register according to the concrete contexts in which 'security' is used" (Huysmans, 1998:228) – essentially, discourse analytic *à la* Foucault.

Following the discursive formation of security within the field of International Relations, Huysmans derives two interdependent forms of security from a particular metaphysics of life located in the cultural tradition of modernity (1998:234): "ontological security, which concerns the mediation of chaos and order, and daily security, which concerns the mediation of friends and enemies" (1998:229). Foucault had also recognized that installation of security mechanisms are intended to bracket the random element in populations to optimize a state of life (Dillon, 2007:44). At the heart of this lies the externalization of death from life, where death is something to be consciously postponed (Huysmans, 1998:245) – a pale spectre that looms in the distance.

Formations of security policy around this externalization of death has the consequence of further desire for knowledge, where death becomes an object we try to know, as well as creating a space within which agencies can appear to mediate and represent our relationship to death. Death, being the ultimate unknown, continually feeds this desire for knowledge. Mediations consist of the 'founding' of objects to concretize danger and those between the self and concretized danger (Huysmans, 1998:237). Security measures can then presume the function of negotiating the boundaries of who to fear (enemies) and who to trust (friends)[4]. This may be seen to have a lucidity-inducing effect on political identity where distinguishing between friends and enemies is seen to constitute 'the political,' distinct from social/economic worlds[5]. This relationship is reflexive, as security feeds the political inasmuch as political identity depends on a definition of 'the other' (enemies from friends) and political actors along the security continuum define further constructions of security. This relationship is also deemed to be unstable in theory in that, were security policies aimed at eliminating threats successful, political identity would in turn be subjugated (Huysmans, 1998:239).

A problem unfolds where strategies of survival/counter-measures assume the possibility of determinability, the result being that 'the void' is hidden by these positive

[4] The concept of trust will be further elaborated on in subsequent sections.
[5] Huysmans draws from Carl Schmitt (1932) here, though this has been taken up more recently by Chantal Mouffe (2005) in terms of the political void created by the search for consensus.

measures that rest on it. This feeds into an *in*security of not-knowing, where state security provisions can be seen as a mediation of both danger and uncertainty. One of the primary functions of the state can then be seen to provide order out of chaos, concretizing dangers/threats to separate friends from enemies, after which identifiable threats can be controlled. This might be viewed as a kind of simulation of order as per Baudrillard, where "simulation refers to the disappearance of the gap between the real and the imaginary" (de Lint, et al. 2007:1635).

Governance through simulation of order is extremely malleable, and could presume to extend its license into perpetuity, as new threats are constructed as quickly as others are identified and enterprises are extended with which to deal with them. As Anthony Giddens has described, as a consequence of conditions in late modernity[6] and the subsequent rearticulation of social relations, "the more a given problem is placed precisely in focus, the more surrounding areas of knowledge become blurred for the individuals concerned, and the less likely they are to be able to foresee the consequences of their contributions beyond the particular sphere of their application" (1991:31). Concretization of dangers can work in tandem with simulations of order/information control (such as the 'demonstration projects' discussed by de Lint et al. 2007) to address the increasing unknowability that has been attributed to life in high/late/reflexive-modern societies, as will be discussed further shortly (though, I would argue, are not necessarily more welcome). Once again however, theoretically, if governments could succeed in entirely eradicating problems outlined in their broadening security efforts, their legitimacy through their capacity to provide order would be at stake.

That such an outcome of this seemingly paradoxical relationship would reach fruition seems implausible considering the proliferation of inchoate fears stemming from the increasing difficulty to ply information into predictable outcomes in high/late/reflexive- modernity (see Bauman, 2000; Beck et al. 2003; Giddens 1991). Jock Young (1998) has highlighted the production of a further obstacle to mediating chaos and order from within the state in the transition from an 'inclusive' to 'exclusive' society. The deviant 'other' who could be easily distinguished in the inclusive society epitomized by

[6] The primary example offered by Giddens is the extension of 'abstract systems' (a combination of symbolic tokens and expert systems) in place of social institutions that have been 'disembedded' - lifted out of local contexts by the distanciation of time and space (1991:17-18).

Fordist work regimes became less distinguishable as market forces created a secondary labour force, transforming the human actors involved through increased uncertainty and job instability, thus creating new subcultures. Reflexively, the market economy cashed in on these new consumer demands, which normalized them into the everyday. The goal was no longer inclusion and reintegration, but marketing to individual desires; hence consumer conformity was replaced by a pluralism of lifestyles. Huysmans posits that such a phenomenon – that of the stranger within the existing order – creates the necessity for ordering to reduce "the possibility for chaos within the existing order" (1998:241).

The ontological insecurities created by strangers (insiders/outsiders who represent ambivalence) are ameliorated by the concretization of danger through risk assessment/sorting technologies where they can be categorized as friends/enemies. He argues that, ultimately, the function of the state system is not to eliminate enemies, but strangers – its legitimacy resting on this ordering capacity (1998:242). This is consistent with Foucauldian literature that outlines the formation of a 'governmentality' that is concerned with the knowledge of uncertainty in governing populations (Dillon, 2007; Foucault, 1991; Garland, 2002; Rose, 1999). This has led to the capaciousness of 'expert' knowledges which seek to create intelligibility and ordering mechanisms through the usage of statistics, accounting, biometrics, and actuarial risk-assessment, each with their own set of truth-telling practices about the knowledge of uncertainty (*creating* semblance of objectivity). Linked with the political, the process of classification is an integral part of social life, both informing and shaping/controlling moral order (Bajc, 2007:1572).

Gilles Deleuze (1992) has contributed to the discussion of the phenomena described above by describing a 'society of control,' different from the disciplinary society of closed systems (described at length by Foucault, 1991) in that it is a system of free-floating complex networks, where individuals in perpetual states of training and re-learning are subject to accompanying ontological anxieties[7]. Most noteworthy within the context of the discussion here is that populations are no longer dealt with in the 'mass/individual' pair, but have become '*dividuals*' within databanks (1992:5), numerical bodies whose access can be regulated with at-a-distance monitoring technologies as

[7] Here I concur with William Walters where he argues that it is better to think of control as a 'diagram' as opposed to a form of society because diagrams are more abstract, leaving open the possibility of other equally valid ways of diagramming the phenomena described by Deleuze (2006:193).

discussed by Richard Jones (2000). Jones coins the term 'digital rule' to describe our regulation of movement through the social world by automatically-generated decisions at various electronic access points (ex: to computer systems or doors that require key cards) that allow/deny access based on the accumulation of digital information gathered at previous access points. He sees this as a new penology in that the exclusion of access can result in similar detrimental effects to traditional punitive measures. Automated gateways or checkpoints that one must pass through in order to participate in various aspects of the social world also require a divulgence of information that might be seen to threaten individual privacy/autonomy (failure to comply equating withdrawal of access privileges – a form of coercive consent).

This kind of monitoring has been a useful tool for rendering strangers into categories of friends/enemies (reducing ontological insecurities). However, we see a further collapse of consent in favour of "information control and its simulation" (as per de Lint et al. 2007:1632). Beyond the immediate implications that monitoring has on trust, security politics can be seen to demand unequivocal amounts of trust from those who rely on the state to mediate their ontological insecurities where there is little transparency to be seen in processes of danger concretization. Both implications will be discussed further.

Thus, an axiomatic understanding of security should be abandoned in favour of situating securities studies within a wider discursive framework of meaning conducive to recognizing its relationship with the political. Governmental rationalities can then be seen to unfold such as those behind a simulation of order to support the concretization of threats/danger, as well as the development of new enterprises to fill spaces created through new technological developments. This approach will allow us "to question our will to truth; to restore discourse its character as an event; to abolish the sovereignty of the signifier" (Foucault, 1971:21).

In the remainder of this paper I will develop this research agenda within the context of internet governance in New Zealand, understood through the lens of 'cyber-security,' and the 'security' signifier more broadly. An examination of the concretization of danger and correlative information management, as well as the development of new enterprises in intelligible order-making will be derived from a complex array of

interviews with participants from varying backgrounds and organisations. Interviews approached security as a theme pertaining to ongoing developments in electronic technology (mainly situated around the internet, critical infrastructure protection, and computer crime). A number of participants were also involved, either directly or through consultation, in the drafting of new legislation that would affect internet governance, or whose positions or experiences allowed them to offer technical or policy-oriented insight into this sphere. It should also be noted that these were collected early in 2002, when 'security' issues were being reified in global political agendas in response to widespread publicity given the topic after the attacks on the World Trade Center in the U.S. on September 11, 2001.

CYBER-SECURITY: SIMULATION OF PERVASIVE THREATS

Peter Grabosky (2001) has posed the question of whether or not 'virtual criminality' is essentially 'old wine in new bottles.' The criteria with which he evaluates this question include examinations of offender motives, interpersonal relations in cyberspace, 'paradoxes of the digital age' (technologies of anonymity and pseudonymity vs. increased threats to privacy due to potential state surveillance of public forums), its transnational dimensions, and responsibilities that come with the potential for computer crimes to implicate third-party liability. Ultimately, he argues that offender motives in cyberspace (greed, lust, power, revenge, adventure, the desire to taste 'forbidden fruit,' and potential intellectual challenges) are nothing new when compared with terrestrial criminal counterparts (2001:243-244, 248) and similarly, that challenges to the state necessitate the same kind of self-reliance that has become commonplace with changing roles of police (2001:245), although "the variety and number of opportunities for cybercrime are proliferating" (2001:248).

While this approach to the question of cybercrime attempts to separate some of the "overgeneralization and hyperbole ... [that] characterizes a great deal of discourse on the digital age" (Grabosky, 2001:243), it does not recognize that there are wider discursive performative functions at work *in the positioning* of 'virtual'- or 'cyber'-crime as separate from traditional crime – that there are specific governmental rationalities instrumentalised under the rubric of 'cyber-security.' Grabosky's approach might be

categorized by Huysmans as a conceptual analysis, yet to yield a further degree of insight and sophistication into the proliferation of cyber-security enterprises depends on the analysis of the signifier within a widening 'security milieu.'

As such, it might be more meaningful to re-visit the question of cybercrime, located as a concern of the broader signifier 'cyber-security' (being an object of cyber-*in*security), and question how its construction as such might be perceived to order social relations. Following from this, though the crimes linked with the concern for cyber-security *do* contain common elements of terrestrial crime, the technological component ('cyber-', which connotes computers and information systems, virtual spaces, and the internet) has instigated new systems that specifically address cyber-security generally.

The importance here is that as long as cyber-security is *perceived* to be an exclusive phenomenon, it impacts ontological insecurities (potential for danger as a result of unknown threats) through its own utterance. This will be shown in the next section where political agendas seek to address this specific issue through the creation of new legislation, and where new enterprises appear that function to concretize danger and control it thusly. A further consequence of a 'security' signifier that deals with the virtual world is the problem of identifying strangers to be categorized as friends/enemies. Due to the complex networks that the internet relies on for functionality and the opaque nature of this connectivity that results, monitoring as a governmental technique is increasingly relied upon to create order out of this seeming chaos, as well as 'expert' knowledge systems that share information to negotiate risks and facilitate aleatory governance.

The following quote highlights the prevalence of governmental rationalities of information control/management; the participant was from the Cyber Crime Forum in New Zealand, in the process of establishing a Cyber Crime Centre for dissemination of information to a broad audience with the goal of being a convenient, single source:

> The worth is going to be in the *perceived credibility* of the Centre and the quality of what they produce. So if they do really good stuff and they have some really good seminars, people will use it and the credibility of the Centre will grow (P10, Cyber-Crime Forum, emphasis added).

What is important is that as long as its credibility is perceived, its existence will be seen as justified – *it need not actually be successful in averting 'actual' crime or keeping dangers at bay.* This highlights the growth of effects-based governance as opposed to

reliance upon original laws as the foundation of governmentality[8]. This can be seen as a practice of rule where success is substituted for legitimacy (Dillon, [drawing from Foucault] 2007:42).

This can also be viewed as an expansion of efforts to govern ontological insecurities versus daily securities, exacerbated by the ominous 'Shadow of No Towers'[9] – the aftermath of September 11, 2001[10] – reaching beyond historically-specific incidence to trespass on the boundaries of time and space, looming overhead and threatening to metamorphose into new (greater) danger at any given moment, potentially close to home. Giddens speaks to this as "the *intrusion of distant events into everyday consciousness*, which is in some substantial part organized in terms of awareness to them" (1991:27, emphasis in original). The media certainly plays an important role here (as shown by Mathiesen, 1997; Urry, 2002); Giddens points out that "the media do not mirror realities but in some part form them" (1991:27).

The provision of 'security' then becomes something like a public relations exercise, where the main challenge is establishing credibility, a theme that was reiterated by interview participants ranging from systems administrators having difficulty convincing management to dedicate money to upgrading firewalls, anti-virus software licenses, etc., to the police in establishing (or expanding) monitoring as a necessary investigative technique, to private security companies in solidifying relationships with their clientele, to the CCIP in establishing credibility as a new government service. Certainly, many of these motivations were contested by other interests (fiscal frugality, protection of privacy, market competition). This often results in organisations seeking matrimony with 'security' to gain acceptance (a heightened political motivator after September 11, 2001), where gaining acceptance and credibility is difficult. A prime example of the staging of such a public relations exercise might be seen through the holding of an Internet Industry Forum; here, legitimacy for the goals of one set of

---

[8] Original laws do, however, contribute to the process of reflexivity that comes with negotiating further laws that would serve as new precedents to be followed, and effects-based governance does not operate outside the realm in which these laws exist (as per de Lint et al. 2005)

[9] This phrase is borrowed from the title of Art Spiegelman's book about 9/11.

[10] Indeed 'after/post- 9/11' was continuously referenced as if to indicate some *zeitgeist*, as a qualifier for a paradigm shift with regard to global security awareness; often this was positioned as "the greater good of the whole outweighs the rights of a few" (P18, Former Market Research Manager, International Data Corp)

organisations was to be achieved by working in tandem with persons from already established organisations such as those within a government body, as the participant notes here:

> P: There was one thing that stood out, was this point about this 'new environment' and that was something that they- they came up with the topic, what they wanted police to go and talk to them about. So that was their terms, if you like, this 'new environment.'
>
> Q: Okay. So they defined it rather than you?
>
> P: Sure, yeah. And I mean, I wasn't going to redefine it so I just, you know...
>
> Q: Did you agree with that general impression?
>
> P: It's probably not completely overstated, but computers have been around awhile and so has the Internet. I suppose increasingly computers are becoming a greater part of our lives. And- but I don't subscribe to the concept of carving off computer crime or cyber crime as distinct from criminal conduct generally [. . .] it doesn't change the nature of the offence. It's just a different [sic] tool for committing the crime. So to that extent they're not new crimes, they're probably new ways of committing old crimes (P19, Crime Policy and Projects Officer, Criminal Investigation Branch).

We can see the irony in this example where the participant admitted that he didn't even personally identify with the term 'new environment' that he was promoting. This may provide a hint toward the extent of informal relationships that are established between the public and private sector (ex: this could potentially be reciprocated by ISPs in informal information sharing to aid in an investigation at some point[11]).

Correspondingly, 'security' was often described as a 'process' of education and awareness by participants in this research project – the 'human factor' being teased out, security even being defined at one point generally *as* 'people.' We can see how 'security as people' is certainly a kind of rationality that epitomizes this struggle for credibility in the legitimization of security issues. An obstacle for security providers could then derive from opinions that New Zealand is *not* a site of imminent danger (ex: for 'terrorist' threats, industrial espionage, etc.):

> Well there's no major threat to New Zealand generated from overseas in the form, you know- there's not [a] great terrorist threat here. There's nobody doing any threat of invasion. So in that sense we don't need to ramp up police and

[11] This was alluded to by many of the participants who worked in investigative capacities within government

> intelligence agencies to deal with the sort of threat that is so limited (P6, Green Party).

One participant mentioned how the corporate culture of New Zealand is even such that any manager who would prioritize security "is quite often seen as being at the bottom of the heap" (P18, Former Market Research Manager, International Data Corporation). Because internet connectivity in New Zealand had not yet developed to the same extent as North America in terms of utilizing the country's available bandwidth (connectivity to perpetually online, high-speed broadband networks was in its infancy), nor did it have the same reliance as in Australia (catapulted by e-government efforts[12]), some participants saw reduced opportunity for related security to be compromised. Many conceded, however, that with increasing connectivity and reliance on electronic networks, technological problems would likely *become* more prevalent (as such, they were not devoid of ontological insecurities about the potentiality of future danger)[13].

Once again, what is conducive to this research agenda is recognizing some of the ways the politics of the signifier 'security' activate to order social relations. The multiplicity of viewpoints represented in the interviews attests to the ability of security utterances to reveal cadences of political identification[14]. The politics of the signifier 'security' can also be seen to activate within different pairings with economic-, national-, cyber-, social-, etc. by participants depending on their motivations. For P6 (Green Party), it was New Zealand's economic security in the face of competition with international markets that was the real issue at stake.

Some participants saw ambivalent attitudes toward security as threatening 'security' itself. For them, New Zealand would become *less* secure or vulnerable if low-levels of awareness were not raised[15]. This sentiment is captured here:

---

[12] This was discussed by P20, Network Security Consultant, E-Crime Solutions.

[13] A brief note to eschew misinterpretation: attitudes toward security greatly varied among participants depending on their politics, professional investment, social experience, and other combinations of factors, potentially ad infinitum. I am not attempting here to make generalized statements such as 'most ISPs promote increased security measures'; the diverse backgrounds of individual participants make this unfeasible.

[14] This also contributes to online communities with shared ethics. A handful of participants went to some lengths describing the different moral codes of hackers (P2), differentiating between 'white hat' and 'black hat' typologies (P30) and vigilante justice groups such as the Cyber Angels (P8).

[15] This was not a universal consensus – for example, one participant interviewed believed that extending government control to deal with security would *create* domestic discontent that would compromise security (P8, Green Party).

> I think you've always got to be aware. I mean, technology's changing pretty much minute by minute [sic] and it's just an awareness that you can be vulnerable. The same as we're always looking for new techniques, new ways of doing things (P8, Department of Internal Affairs, Censorship Compliance Unit).

As such, resources are actually invested in *raising* ontological insecurities through 'awareness' measures, in turn legitimizing the functions of various 'security providers.' Incorporation of the 'security' signifier in dealing with technology or digital information-related problems has helped to politicize particular issues, heightening their perceived worth. One participant working for a major global player in the computer security industry admitted that there is a 'big hype' where a lot of computer security companies "create fear, uncertainty, and doubt around computer security because it sells their product." At one point, he went as far as saying:

> We have to perpetuate the myth that all of these vulnerabilities are going to be the end of the world for you (P17, Team Leader, Information-Assurance Services Security Delivery, 'X Company'[16])

Going into this further, the participant justified this is as a matter of perpetuating the status quo – that clientele are already interested because they might have recently read about a particular threat in *Computerworld* or watched it on CNN – and his business just does what another security provider would offer anyway, but at a more competitive cost. That the participant's company purportedly did not seek out *new* clients by instigating these insecurities may not affect much though, this being one of a number of private securities providers who noted a cultural shift in thinking about security, facilitated in large part by the media.

Mathiesen (1997) has described how dramas are staged to promote particular societal values, political agendas, etc. He calls this 'synopticism,' where the many watch the few; in composition it is diametrically opposed to Foucault's iteration of Jeremy Bentham's 'panopticon' (where the few watch the many), yet similarly, it is an ordering mechanism. Synopticism is a useful tool in the simulation of order. It may be seen here where participants drew on sensational examples to offer justification for 'security' practices specific to their interest, or noted an awareness of such things in media discourse.

[16] This participant requested that the identity of his employer remain anonymous, 'X Company' being the chosen pseudonym.

For example, the Mark Lundy murder case[17] was drawn on by participants within the police service to highlight the forensic value of computers in solving 'traditional' crimes. Obviously, someone murdering their wife and daughter is not of the everyday, but its dramatic effect can be useful political fodder. Information-sharing, a vital part of police work, was seen to hinge on public perception of police credibility. A deficit in public willingness to respond or provide information to police based on a lack of understanding of what's required in doing police work was reflected on here:

> But it's also the willingness of these particular entities, for ISPs or Telcos[18] or who it might be to provide us with information – banks, power companies, local authorities, you know- a whole range. And information is what police trade on. It's what we- if you haven't got information you get nowhere. If we can't get it, we have no job. I don't think that really they can see with the difficulties, the changing environment around getting it (P19, Crime Policy and Projects Officer, Criminal Investigation Branch).

That "information is a commodity" (P21 E-Crime Lab, New Zealand Police) was a recurring theme (especially with respect to the importance of 'human intelligence') underlines how synoptic media valuations of police effectiveness are paramount to their success. Another example of the employment of synopticism, here to concretize danger, was where media coverage of the 'cyber-stalking' of children was conceived as intensifying political debates about drawing the line over freedom of expression and freedom of access to information, situating it in favour of a particular political agenda (P1 from the Council of Civil Liberties).

Indeed, media characterization of potential threats was seen by some to have already translated into an effect on cultural perceptions of cyber-security. One participant noted that although the same vulnerabilities are coming out, the "level of security of organisations has changed," seeing this as a change in culture (P30, Security Consultant, Deloitte Global). While this feeds into ontological insecurities (in mediating precedents with which to negotiate the potential for future calamities), it does not actually offer useful solutions, ergo:

---

[17] Mark Lundy was convicted in April 2002 (his trial in progress during the interview collection) of murdering his wife and daughter in August 2000 – this is noted as one of the more complex and controversial trials in New Zealand's history. Computer forensics were lauded as a key component in the conviction whereby it was found that the clock on Lundy's computer had been manipulated, indicating premeditation.

[18] This was a commonly used abbreviation for Telecommunications Companies.

> The community at large is not well-informed or educated onto cyber issues and the press don't help, particularly because they tend to dramatise what does happen without- they give us the bad news but they don't tell us how to stop it (P10, Cyber-Crime Forum).

A common conception among computer security professionals interviewed (network/system administrators, private security providers, and independents) was that security was a 'process,' and thus can never be fully realized. Important to them was that at the end of the day it was perceived that they did the best they could, noting the impossibility of reading up on all emergent vulnerabilities. Here is an example of the impossibly wide expanse within which provision of computer security may be negotiated within the context of system maintenance:

> So rather than just saying 'okay it does all it's supposed to do' you have to look at [it] from 'does it not do what it's not supposed to do.' So it's kind of looking at [it] in the negative. (P30, Security Consultant, Deloitte Global).

Between mediated presentations of insecurities and the simulation of ordering ontological threats around concretized dangers, things could be seen to get confusing for laypersons. With regard to customers phoning into their ISP regarding computer problems:

> There does [sic] tend to be a few problems that are more, perhaps perception-based rather than actual reality, and so there's a reasonable amount, because technology is not necessarily all that well understood (P14, Network Administrator, Com Net [Industrial Research Ltd]).

One further aspect of the simulation of cyber-security, which will tie into the next section, is that simulation as might be seen effected through the introduction of 'piecemeal legislation' to deal with perceived computer threats may be a result of the reflexivity that occurs in 'law's shadow.' Here "the reflexivity of law is understood [...] with the requirement that justice may also (simply) *appear* to be done as an iterative process, the last word of which may usefully be deferred for utterance elsewhere" (de Lint et al., 2005:69, emphasis added). Hence a seemingly incomplete set of legislation might be pushed forward to immediately respond to politicized issues, though it may be of little use in actually alleviating problems (or may proceed to create new problems as a result of inadequate consultation). That it is perceived to address the issues legitimates its existence, though further amendments could be necessitated after the fact.

This resounds with a common complaint about much of the existing software architecture where security is not 'designed in.' What is being suggested there is that contingencies for ontological insecurities have to be built into new systems – problematic if one is not able to accurately predict the future. Hence, open-source operating systems (such as Linux and UNIX®) are lauded for the benefit of being open to improvement by users, something closed-source systems (such as Microsoft operating systems[19]) do not allow.

NEW ENTERPRISES IN INTELLIGIBLE ORDER

As noted by Anthony Giddens, "expertise itself is increasingly more narrowly focused, and is liable to produce unintended and unforeseen outcomes which cannot be contained – save for the development of further expertise, thereby repeating the same phenomenon" (1991:31). This has been shown to be the case with the example of closed-source software design where contingencies have not been designed into the architecture, and with New Zealand's Crimes Amendment Bill No 6, viewed here as:

> [...] a piecemeal approach which tends to be somewhat knee-jerk to particular problems or perceived dangers or perceived needs. And in some instances, not just at a legislative end but also sort of quasi-legislative regulation or other areas which [sic] have a loose sort of feel about them – codes of practice and so on. They're completely inconsistent (P22, Internet Society of New Zealand).

As mentioned earlier, a governmentality favouring effects-based policies and practices where merit is bestowed based on *perceived* worth (as opposed to actually *doing* 'justice') often results in deferral of the last word to some indeterminate time in the future. The contestation that may result from unsatisfactory results in the interim may lead to new enterprises with which to deal with these problems.

Drawing again from the example of the Crimes Amendment Bill No. 6, it must be noted that this legislation did not occur in a vacuum. It was, in part, a response to existing legislation that was too narrowly focused to empower police with the ability to prosecute computer-related crimes such as denial of service attacks and theft of electronic

[19] Microsoft's system of recognition of dealing with information provided to them by third parties identifying 'bug' fixes and potential backdoors into their OS was discussed by P13, an Independent Security Consultant.

information (not encompassed in the definition of property in previously existing laws)[20]. Police were not investigating electronic crime because there were no laws to create demand; once again, this returns us to the notion that perceived worth is a cardinal concern. Cyber-crime was seen as contributing to the 'dark figure of crime' – that of unreported or undiscovered crimes that don't make their way into official statistics (P19, Crime Policy and Projects Officer, Criminal Investigation Branch). This feeds into discourse within police services where computer crimes were seen to be comprised only of traditional offences that made use of 'new tools,' or where new usage of computers was primarily associated with utilities to be incorporated into forensic work for traditional offences.

In the meantime, this allowed private securities companies to thrive on the legal loopholes – to provide services that the police couldn't offer. In New Zealand then, the private sector was often relied on to determine which security threats rotated the world of cyber-space, and it was often the first line of defence. Private companies did, however, face their share of challenges in the process:

> [...] you're hindered in the private sector to do a thorough investigation because the law is [sic] at the moment keyed up to the [sic] law enforcement like the police and various government agencies. And albeit it [sic] now they're not doing their job, hence it's creating a market in the private sector, but the laws aren't sort of open to the private sector yet to let us do the work (P27, E-Crime Investigations, Corporate Risks).

Working within the confines of the law, the private sector relied on the auspices of the state for certain investigative procedures such as search warrants of an individual's private residence[21]. It was interesting to note that private firms could file for search warrants through the same channels as the public police, following through on the necessary paper work, to the point where the search warrant was granted. At that point, however, the investigation would be handed over to the police who were singularly empowered by the law to serve warrants, limiting private investigators. Even then police

---

[20] Returning to the earlier discussion about whether or not cyber-crime can be differentiated from traditional crime, these legal discrepancies are shown here to order social relations in distinct ways.

[21] Private companies were usually able to bypass the search warrant process at the site of their employer/client because if the client had jurisdiction over their property (as was often the case), access could easily be granted. This was aided in cases where an employer had a computer use policy wherein it was stipulated that all data transpiring on workplace computers was property of the employer (worker access privileges contingent on consent), implications as discussed by Jones, 2000.

would sometimes defer serving a warrant (though already lawfully validated) until convinced that certain criteria had been met to justify their involvement; this criteria was that a search warrant would likely lead to a conviction.

Because the police were of this prosecution mindset, work in the private sector often better complemented situations where the goal of clients was *not* prosecution (due to perceived public relations repercussions concerning a breach within their company, sensitive information surrounding a case, time and money, etc)[22]; private security contractors did not depend on prosecution as a measure of success; this was more a matter of whether or not the client had perceived that they had fulfilled their function[23].

The police position as principal investigator is still legitimized through state legal constructions, while at the same time allowing significant diffusion of resources through private sector alliances. This creates further opportunity for public-private partnerships, namely the establishment of informal information-sharing networks – for police, access to information garnered by the private sector that waives the need to spend time wading through legally-prescribed bureaucracy; for the private sector it is often much the same – the relationship is reciprocal. Strategic alliances may also be formed between agencies with similar motivations or political agendas when legitimacy is at stake, as shown in the previous section.

Where legislation was languishing, security contractors were seen to prosper in the field of computer-related crime. This phenomenon will likely continue, especially in the highly-contested space surrounding 'security' issues because of "the accelerating speed and the unprecedented magnitude with which new technical artefacts are developed and moved to market, and with which new forms of knowledge are fabricated" (Stehr, 2003:643). Due to the lengthy periods of time it takes for new legislation seeking to adequately address perceived emergent threats not dealt with in existing laws to be

---

[22] In this, the computer-related crimes discussed here are similar to 'white-collar' and corporate crimes, where the private sector is called on instead of the police. In interviews with participants in police services, it was noted that such crimes (white collar, bank fraud etc) were usually absent from discussions of 'traditional' crime or policing concerns, even though they are surely more prevalent than murder, which frequented the lips of participants.

[23] Noted by a participant in the private security industry focusing on 'electronic crime,' they *do* balance what's worth investigating based on statistics, though the perceived potential for success is not limited to prosecution potential but determined by the client's desired outcome, often to find out how a security breach was made to inform future prevention (P27, E-Crime Investigations, Corporate Risks).

enacted, new enterprises will emerge to meet market demand. This is consistent with the often-iterated prediction among participants that the internet would become both more secure (where security technologies were improving) and less secure (where there emerge more imaginative ways to abuse it). One participant likened this to climbing two sides of a pyramid, where it was undetermined whether you would get to the top or not (P10).

Nico Stehr has stated that "an analysis of the governance of knowledge in modern society has to be cognisant of the general practical incompleteness, fragility, obsolescence – and often, failure – of projects aimed at governance in modern societies" (Stehr, 2003:645). Certainly governance of electronic crime in New Zealand was seen to be highly contested, and the legislation that was being established at the time of the interviews discussed here seemed destined for revision in the not-too-distant future due to a number of perceived problems.

Some of these problems were believed to arise from a lack of transparency in the drafting of legislation. It was purported to be extremely difficult for citizens to access a copy of the Supplementary Order Paper for the Crimes Amendment Bill No. 6 (ex: it was not made available online), and was badly promoted in terms of the consultative process, relying solely on the knowledge of a select committee. After considerable efforts to gain access to the consultative process of the Supplementary Order Paper (having to constantly monitor various places to keep up to speed with the legislation), the Internet Society of New Zealand helped effect the addition of two new crimes[24]. Unfortunately they included very wide provisions such as seven years' imprisonment for Denial of Service attacks. For these, there was no opportunity for formalized debate before they were presented to the House. Eventually, they were able to get one word changed[25] (P22).

That drafting of legislation was closed to specific groups did not seem to be out of the ordinary. For example, the Consumer Protection Bill sought consultation from the Ministry of Economic Development (MED) who were concerned with copyright protection. As such, private agendas are summarily concretized in law. The consultative committee for the Crimes Amendment Bill was comprised primarily of police, the Internet Safety Group (concerned with child pornography), and the largest ISPs

[24] It was not clear from the source what these additional crimes were.
[25] Once again, it was not clear what the wording was specifically – its inclusion here is to capture general concerns participants had with the legislative process.

(Yahoo!Xtra and Clear Communication Ltd.); beyond that, most ISPs were not involved despite potentially crippling economic burdens the legislation could impose on them. An example is that the Telecommunications Interception Capability Bill (a companion bill to Crimes Amendment Bill No. 6) criminalizes network operators' failure to provide clean interception capability (log files) to assist with police investigations[26]; this would require allocation of substantial resources just to *store* the log files for a minimum period of time, shown to be a huge cost to ISPs in the UK with the exercise of the Regulation of Investigatory Powers Act (RIPA). It was perceived that this could also create a dampening effect where costs would be passed on to consumers, especially if police felt compelled to employ interception powers pre-emptively and with more frequency fearing that data might soon be wiped[27]. Neither was the Minister of Justice's response to these concerns ('don't worry, the police would never prosecute [ISPs]') seen to be comforting (P22).

A further concern was that the Consumer Protection Definition of Goods and Services Bill sought to change the definition of goods and services under, in particular, the Consumer Guarantees Act due to a particular court decision ruling that electricity was not a good and its supply was not a service, and therefore wasn't covered by guarantees given to consumers under that act. One participant commented on how this reading of the legislation didn't respond to the way people normally think about goods:

> [...] it will dictate that anything carried over an electronic network effectively is a good, and that its delivery is a service. And effectively that's all they've done. And what that means is when you slot those definitions into the Consumer Guarantees Act [sic] the guarantees are for things like 'it's got to be fit for the purpose, you've got to have clear title to it,' – in other words, you've got to own it in order to sell it. It's got to be safe... of reasonable quality. Now how on earth do you fit those guarantees into the delivery of an email? (P22, Internet Society of New Zealand).

Once again, it was of the opinion that little technical specialist input was received before the legislation was drafted – rather, it came about in response to perceived problems.

In direct opposition to the Crimes Amendment Bill No. 6 was the Telecommunications Privacy Code, the result of efforts from the Privacy Commissioner

---

[26] This bill also gives the Security Intelligence Service (SIS) and Government Communications Security Bureau (GCSB) the power to intercept emails.

[27] Demonstrating a limited timeframe within which an investigation could be carried out was seen to help expedite the warrant process (P19).

to try and balance out what he perceived to be threats to civil liberties as a result of the increased monitoring capacity that was being given to police, the Security Intelligence Service (SIS), and the Government Communications Security Bureau (GCSB). He was, however, seen to be simplifying the problem by moving the boundary back a step further in proposing that ISPs be required to remove traffic information permanently after six months. The problem here was seen that as soon as a period is specified, it may be too long (where ISPs can't keep huge amounts of information due to cost) or too short (for law enforcement purposes). Of significant worth here is that there was seen to be a high degree of exceptionalism in singling out ISPs and Telcos from other industries that hold customer information potentially as useful to police investigations, such as banks, insurance companies, and travel agents (P22).

This legislation can be seen as the result of efforts to address potential threats loosely related to 'cyber-security' along a diverse array of political agendas. The desire to deal with ontological insecurities of 'not knowing' are implicit in Crimes Amendment Bill No. 6 where the monitoring capacity of the GCSB was extended, which could potentially aid with the categorization of strangers (chaos) into friends/enemies (order) and thus, be dealt with[28]. In contrast, the Privacy Commissioner was attempting to remove the possibility of not knowing whether or not one is being watched by stripping government agencies of the tools to do so. Cyber-security was activated here as a political motivator, instigating wider definitions of terminology used within legislation. This could be seen as an application of what Martin Innes refers to as 'control creep,' where social control apparatuses have been used by governments in a way that "progressively expands and penetrates (or 'creeps') into different social arenas," in response to vague fears about security in late-modernity (2001:1).

In addition to legislation put forward to deal with these issues, a number of other enterprises could be seen as aspiring to contribute to concretization of danger, such as the creation of a Cyber Crime Centre (discussed earlier within the context of simulation) and, most notably, the newly conceived Centre for Critical Infrastructure housed within the

[28] The GCSB's function has been described generally as spying on other countries (P5, Independent Watchdog), more specifically, through the interception and analysis of foreign communications (de Lint, forthcoming), and also the monitoring of the foreign element within New Zealand (P1, Council of Civil Liberties). In essence, concretizing danger and stripping the stranger of anonymity – possibly *the* enterprise in intelligible order-making in New Zealand.

GCSB – a 'watch and warn' service with a mandate to assist in the protection of New Zealand's national critical infrastructure from information-borne threats (de Lint, forthcoming). These might appear redundant considering there are already a number of related services in widespread usage (such as CERT®[29]), and yet their legitimacy was accepted by participants as contingent on future perceived worth. It seems unlikely that resources would have been deployed for these programs were there not sufficient ontological insecurities running amok with which to face.

As Giddens has noted, "Expert knowledge does not create stable inductive arenas; new, intrinsically erratic situations and events are the inevitable outcome of the extension of abstract systems" (1991:31). It is within these new arenas, with their erratic situations that new projects to deal with insecurities are created. New industries emerge here to thrive in gaps of seeming unintelligibility to restore order or address perceived problems; in many cases this is merely an exercise in simulation of order where knee-jerk reactions are not seen to contribute to long-term solutions. As was demonstrated previously, unknown dangers often become misrepresented through concretization (hype) in order to aid in perceived credibility and public acceptance (in many cases to promote a 'security' product). Transparent in this process is the fact that knowledge with relation to security is highly tenuous, and because of the limitless scope of potential security concerns, it is unrealistic that one provider should presume ownership of any semblance of 'complete knowledge' about potential security issues, as captured by this participant:

> So there are probably always going to be things that I don't know about that someone else may find that- and that just comes with the territory, and that's- that's just, you know, something you have to live with you know. I mean, you're never going to find everything – you can try and do is raise the level of security to a standard that's, you know, good enough for them (P30 Security Consultant, Information Security Services Team, Deloitte).

Because of the insurmountable scale of existing information pertaining to security knowledge, citizens must allocate increased levels of trust in security professionals and third-party sources. This will be discussed in the following section, along with the relationship between trust and monitoring, used as a tool to channel ontological insecurities.

[29] Computer Emergency Response Team

ONTOLOGICAL INSECURITY, TRUST & MONITORING

As previously mentioned, following the transition from an inclusive modern society that reached its pinnacle with Fordist work regimes to an exclusive society typical of a high/late/reflexive- modern era (see Young, 1998), comes the intensification of 'the stranger among us.' This was seen by Huysmans (1998) to be a challenge to the state whose legitimacy rests on its capacity to provide order, the stranger being an unknown element – an insider/outsider - having an inimical relationship with the process of this order making. Strangers must be identified before the categorization of friends and enemies can proceed. As such, monitoring is seen as an indispensable asset in this capacity.

Giddens has outlined an unyielding exchange between monitoring and trust, whereby "trust presumes a leap to commitment, a quality of faith which is irreducible. It is specifically related to absence in time and space, as well as to ignorance. We have no need to trust someone who is constantly in view and whose activities can be directly monitored" (1991:19). This 'trust leap' is elaborated on by Guido Möllering, where the leap of faith from the kinds of weak inductive knowledge[30] that inform some state of favourable expectation involves a 'suspension' of time and space that serves to bracket the unknowable "thus making interpretative knowledge momentarily certain" (2001:403). Möllering develops this further, positing that 'suspension' cannot exist independent of interpretation, and that, "if suspension emphasizes the illusory and indifferent character of trust [...] this is balanced by the continual and reflexive nature of interpretation" (2001:414).

Bringing this into Huysmans' discussion of security, monitoring is intended to reduce ontological insecurity and anxiety (fear of not knowing) by reducing the *need* to trust, giving further meaning to the expression 'keep your friends close, and your enemies closer.' Monitoring becomes self-reflexive where there is an element of trust

[30] Möllering's main source is Georg Simmel, also drawn on by Giddens. Though the importance of the 'leap of faith' is expanded by Giddens through his discussion of the nature of the leap to commitment, particularly his notion that we don't *need* to trust what can be monitored, here 'visibility' tends to overshadow the interpretation of 'good reasons' and how this is translated into expectations. Though monitoring can certainly remove some of the ambiguities which necessitate the element of faith, as well as provide a *basis* for interpretation, it does not address how "interpretations do not translate directly into expectations" (Möllering, 2001:415).

invested in the practise itself, particularly when its means of determinability is evaluated. The favourable expectation of making ambiguities known invokes a quality of faith toward this end result (where time and space is momentarily suspended), so monitoring must be turned in on itself in order to evaluate its merit (to 'monitor monitoring,' so to speak). Of course, there is always some ontological insecurity when attempting to predict the future (due to the inability to realize every potential unknown), and so the process of monitoring, in terms of its relationship to trust, is doubly linked. Theoretically, the paradox of monitoring in this capacity is realized where, if all ambiguities were to be revealed through its efforts, it would no longer serve any useful purpose.

As was shown to be the case with systems administrators who relied on 'watch and warn' bulletins and newsgroups to secure their networks, trust played a role where they needed to monitor vast sources of data to keep up with knowledge. The monitoring function served to alleviate the *need* to rely on the kind of trust described by Giddens, yet as was noted, they could never be *fully* informed, thus, needing to trust that they did all they could do at the end of the day. Trust is pronounced here again where they negotiated which security services to subscribe to – this was usually influenced by reputation (presence in the media, review sources, standing within trusted networks, etc) or business relationships that their organisation actually had with these services; in both cases, visibility is a factor. Security professionals also avoided services that did not provide frequent updates, so as to limit the need to prolong suspension of trust (that viruses or systems intrusion will not occur in the interim) or for further reliance on trust (consequent to initiating relationships with new security providers). We can also see here how this relationship between monitoring (visibility) and trust would be an important aspect in enterprises' vying for public credibility (and so synoptic practises proliferate).

Tying trust into the previous discussion of the sphere within which 'security' enterprises can emerge to alleviate ontological anxieties, we can see their success potential elevated by increased needs of the layperson to rely on trust where the enormous scale of information available about potential dangers is coupled with the unlimited unknown of potential dangers themselves; this does not allow for any deficit of trust. Once again, Giddens observed that "[i]n respect of expert systems, trust brackets

the limited technical knowledge which most people possess about coded information which routinely affects their lives" (1991:19).

As was remarked earlier, the legitimacy of the state often rests on its capacity to provide order, contributing to the definition of friends and enemies, constructed alongside particular political agendas. The element of ambiguous threats is then both a challenge to order-making while at the same time, of crucial importance to ensuring further demands for these efforts. Ambiguous threats that are seen to be borderless ('terrorists,' hackers, cyber-stalkers) can be represented as both national and domestic security issues. Outsiders/insiders who bear the visage of the stranger must first be seen as either friends or enemies before they can be dealt with through monitoring techniques. Expansion of the GCSB's monitoring capacity, as well as its ability to intercept communications of foreign elements within New Zealand[31] (with only ministerial oversight, thus subject to partisan political bias) could be seen as an example of how the foreign (stranger) is viewed as a potential enemy that needs to become known.

Aside from the monitoring of 'the stranger within and without' by the GCSB, police services relied on a moralistic hierarchy to determine who should be the subject of monitoring, and for what kinds of crime. This was, in large part, due to resource restraints where there were only 6,000 police officers in a country of almost four million people. As one individual noted, "it is only used for the most serious crimes" (P19). An example can be seen with the monitoring done by the Censorship Compliance Unit, concerned with online traders of child pornography.

Relevant to its discussion is Charles Tilly's position that centralized governmental regimes actually *depend* on 'illicit trust networks' (such as those formed on the internet) for actual execution of top-down plans (2004:15, also see Holquist, 1997). Since networks generally operate within existing social or systemic archetypes, regardless of the beneficence of this relationship, they can be prone to surveillance from others with access to these systems. The employment of computerized surveillance to identify potential threats was the primary resource tool for the Department of Internal Affairs'

[31] The defined parameters were so broad as to provide means to capture within their gaze companies that are part of a corporate body or its subsidiary incorporated outside NZ, companies that have controlling shares in other countries (including foreign-owned banks), unincorporated bodies that are part of foreign organisations (which could include trade unions), and persons acting in their capacity as an agent or representative of any government, body, or organisation as per those examples just outlined (P1).

Censorship Compliance Unit, which was primarily concerned with eradicating child pornography from the internet. The investigative monitoring techniques of this organisation are summarized by this participant:

> What happens, we got onto a channel and there may be, say, fifty people from all 'round the world and there may be a couple of New Zealanders flat-out trading. What we try to do is to encourage them to send us material. We're in a public area. There are [sic] no entrapment issues because all you're doing is getting them to do what they normally avail themselves to do. In the majority of cases we get approached by them. (P8, Department of Internal Affairs, Censorship Compliance Unit).

That the participant described the Censorship Compliance Unit's interaction with participants as getting them to do "what they normally avail themselves to do" should not go without comment; it denotes a pre-emptive rationale consistent with other participants who employed surveillance techniques, which rests on the underlying insecurity that an offence looms in the future. The perception of *mens rea* (guilty mind) is often enough to legitimize the employment of monitoring[32].

There seemed to be a recurring in-group/out-group discourse prevalent among many participants that stated monitoring was a large part of their work, which could potentially be attributed to the mentality that is required for the task (looking for 'others'). Often these participants mentioned that they were frequently engaged in information-sharing practices within networks of similarly-tasked people, sometimes hesitant to rely on support outside of these groups. An example here is that the Censorship Compliance Unit did not use any external contractors for their own computer security, rather, they relied on information from similar enforcement trust networks, where problems were posted in group forums and someone within the group would suggest how to come up with a solution. Another example of trust being conferred based on perceived common interests is where a private investigator mentioned that all of their staff were ex-police, however, once they left the police service, they were no longer trusted (P25, E-Crime Investigations, Corporate Risks).

Neither did there seem to be a great deal of trust toward agencies that monitor communications among other participants. The GCSB was often referred to as a 'spy

[32] This is not intended as a criticism, just observation (another observation is that this has not proved itself as an effective preventive technique, especially where the participant indicated that they often find themselves serving search warrants on the same few individuals).

agency,' and some participants expressed concern that the CCIP would be located within its wings. From the perspective of the CCIP, it was seen that being tucked within a branch of the GCSB could come with the benefit of access to many of the GCSB's resources. Within the context of this discussion, a potential strategic benefit could be that this might expedite the perceived credibility of the CCIP for foreign governmental agencies who have a relationship with the GCSB, helping to facilitate information flow[33]. Also, from a public relations perspective, were the CCIP to be revealed in the eyes of the public as existing for a shared common good (ex: New Zealand's critical infrastructure), it might help to alleviate some of the negativity compounded for the GCSB over the years (for examples, see de Lint, forthcoming).

Further problems experienced in monitoring practises stemmed from the result of the opaque nature of connectivity on the internet. Encryption technology has become more widespread in response to growing fears about privacy and data mining, inhibiting investigations[34]. There is also an element of trust that has to be allocated to the perceived reliability of digital signatures where the identity of the person who supposedly originated the signature can never be truly known, tying into concerns with rampant online fraud. An additional challenge faced by enforcement agencies in dealing with computer crimes was that they had to place individuals at the scene of the crime, which was particularly difficult in cases where there happened to be multiple users. One participant conceded that at the end of the day, all they really have to rely on is circumstantial evidence.

Though the GCSB, SIS and police services of New Zealand were allowed unprecedented interception and monitoring capabilities through the Crimes Amendment Bill No. 6, government agencies did not hold a monopoly over the identification of

---

[33] In response to whether or not they have a memorandum of understanding with other agencies, a participant from the CCIP said "No, it's the fact that we're part of the club, I guess. Having established the CCIP here they see that as an equivalent organization and they're quite happy to exchange with us" (P23).

[34] There was actually a debate occurring amongst participants about encryption/decryption. From an enforcement perspective, encryption was seen as a tool used by criminals to mask their identity when committing online crimes, whereas to some security consultants, encryption was a useful tool for protecting against online info/identity theft (credit cards, etc). There was also talk about whether or not it should be an ISP's responsibility to provide police with decryption tools; from an enforcement perspective, it was thought that ISPs have a 'social responsibility' for crimes that their network helped facilitate (lack of police resources feeding into this), whereas from an ISP perspective, forcing them to provide such tools would also come at great costs, referencing the exclusory principle of holding ISPs responsible (ex: police don't hold telephone companies responsible for crimes that their phone lines may have helped facilitate).

potential threats with which to concretize danger, nor were they seen to be the most active contributors to provision of 'cyber-security,' particularly with regard to electronic crime (as a result of the legal limitations outlined earlier[35]). Systems administrators and private security companies were also actively involved in this line of work, and thus often relied on forms of monitoring before they could concretize danger or identify the source of a perceived threat.

As such, they were also subject to many of the same problems, especially because the internet is essentially a borderless entity, where remote access can be established from anywhere globally, and where the e-crime is transparent in nature. When securing networks, a major problem was how to let in the 'good guys' and keep out the 'bad guys' (P17). Intrusion detection systems were set up to monitor activity on networks and servers, as well as programs to monitor workplace computer stations; however, according to participants it was impossible to monitor all activity due to sheer scale. The following quote exemplifies these issues:

> P2: Yeah, we're keeping track of some of the things, like file access and who's [sic] deleting files and all that. Things like dialling up from home or remotely – that's all being logged.
>
> P1: Web access is logged.
>
> P2: Yeah, all the web access. All access to our servers is logged as well and the firewall logs – all the traffic in and out, anyway.
>
> P1: Too much to read through.
>
> P2: Yeah, it's way too much data to read.
>
> P1: It would only be if an incident happened to someone.
>
> P2: You'd be able to trace it back.
>
> P1: What- what happened then- it would be our job to try and find out.
>
> Q: So you basically log all that stuff for forensic purposes rather than actual monitoring?
>
> P2: No. We're supposed to be monitoring it as well- it's just that we don't get time and so a lot of it ends up for forensic purposes later in, yep (P3, System Administrators, 'Government Department').

[35] The Censorship Compliance Unit would be an exception here because their work concentrated on public forums.

Many companies were seen to be moving towards adopting computer use policies stipulating that any data on work computers would belong to them. This helped to facilitate monitoring by private investigators and systems administrators without the need for search warrants. The steering of information flow through specific channels, password usage at workstations, pre-registration with systems administers who regulated different levels of user access, compartmentalization of critical data and the regulation of physical access through use of electronic key cards were all techniques employed to varying degrees to reduce reliance on trust[36].

To sum up this section, monitoring was seen as a tool to filter ontological insecurities into recognizable categories of friends and enemies. This was shown with the GCSB's increased capacity to monitor foreign elements within New Zealand. The practise of monitoring has a direct effect on trust, where monitoring is used to decrease reliance on trust for those who employ it. Because of the opaque nature of the internet and increased user anonymity, monitoring becomes more difficult but is employed more regularly to decrease this trust reliance. Information pertaining to security is often handled by organisations that have little organisational transparency, especially with regard to monitoring practises, and this also creates an increased reliance on trust. Trust networks that facilitated flow of information between similarly-tasked organisations were also shown to be present. Policies and practises within organisations reflected ontological insecurities about perceived future unknowns and incorporated the means with which to monitor employees, also employing various means with which to regulate access. But the questions remain: is the effect that potentially being monitored (ex: by the GCSB) has on others' ontological security worthwhile? Conversely, does having to place more trust in organizations with little transparency in their securitization practices eliminate ontological anxieties? Do these lead to harm reduction? These questions will be explored in the following, final section.

[36] For a further discussion of the implications of these practises, see Jones, 2000.

SECURITY POLITICS: AT ODDS WITH HARM REDUCTION?

Before concluding this examination of security, let us give brief pause to the nature of (security) knowledge itself. It has been argued that equating 'information' and 'knowledge' bypasses the issue of trust, knowledge being "information that can be trusted," whereas information alone is as yet undetermined and unfiltered (Brodeur and DuPont, 2006:11). The general argument is worth noting, though it could be better resituated within the aforementioned discussion of trust. Undetermined and unfiltered information should then be seen as that which has yet to be allocated an expectation to inform the interpretative process involved in the mental process of trust, whereas knowledge may be seen as a suspension between interpretation and favoured expectation. This accommodates the notion that 'knowledge' can be highly capricious, vulnerable to collapse in the event that expectations are not met. It is only a suspended commitment that bridges the gap between knowledge and ignorance. Thus discursively oriented, it sheds light on the following:

> You've also got to be quite careful about creating – what would be the right word to describe it – if a lot of people say it's so, then it becomes fact. So if one person says 'okay I've seen this vulnerability' and it gets passed around, suddenly when it comes back you say 'yeah, that must be right, if he said so.' It may [sic] be incorrect. So there's a phrase to describe that (P10, Cyber-Crime Forum).

The wariness this participant had with regard to the self-reflexive nature of adopting potentially untenable foundations on which knowledge about security vulnerabilities are constructed is interesting. Many participants shared the sentiment that information about security cannot necessarily be trusted, a rational standpoint considering the limitless scope of what 'security' might entail, and depending on whose interests are at heart in its fabrication. Contributing a specific vulnerability to public discourse can create precedents that, once concretized (politicized), can impede further discussion. This can also contribute to processes that substitute deferral for the last word.

Willem De Lint and Sirpa Virta (2004) have argued that security should retain a semblance of ambiguity to promote harm reduction by reducing the ontological *in*securities that have been fostered in political agendas, consistent with Foucault's notion that "the operation and proliferation of mechanisms of security continually inflated the concern with security" (Dillon, 2007:45). De Lint and Virta posited that there needs to be

"a rejection of the association between security, certainty, and authority" (2004:465), where defining security as a particular problem narrows the realm of contestation and debate known as 'the political,' as was discussed earlier. Many participants also suggested that if security is too narrowly defined, other problems, potentially as important, could be overlooked. The lack of transparency involved in negotiating security threats before they are filtered to the public creates an increased reliance on trust that 'the experts' know what they're doing. The politics of the security signifier often activate to propel 'security' issues to top priority, yet, as the following participant noted, create further secrecy surrounding such issues:

> [...] stuff that is inherently open becomes tainted by security simply because anything that security touches has to be considered secure and confidential (P28, IP Architect, Telstra Clear).

In this way, security issues have been likened to investigative police work (as opposed to preventive techniques) where 'you can't say too much too soon' (P10) and the surrounding area has to be locked down to protect the chain of evidence from contamination. The drawback of this was seen to be that warnings for problems weren't coming out fast enough (P10).

Buying into a security agenda whereby there is fear of some ambiguous external threat can be seen to encourage a license into perpetuity for means with which the state can unmask strangers at home, ordering citizens into categories of friends and enemies that can then be regulated (through control of mobility). Thus, the intra-state practices that follow from security agendas put forward by governments serve to both alleviate ontological insecurities that come with unknowability (strangers), while legitimizing the state's ability to create perceived order. This was demonstrated though the increased monitoring capacity of the GCSB in New Zealand made possible by the Crimes Amendment Bill No. 6 and Supplementary Order Paper No. 85. The Associate Justice Minister, under whose aegis this legislation was promulgated, was widely reported in the media as saying that 'law-abiding New Zealanders have nothing to fear from the proposals' (P1).

As Lucia Zedner has observed with regard to the marketing of security products, "far from alleviating the fears that led to their purchase, these products provide users with daily palpable reminders of the very risks they seek to avoid" (2003:165). In relation to

fears about electronic threats, this can be applied to the usage of antivirus and spyware protection software. As was shown earlier, it is these types of ontological insecurities however that create the spaces within which security providers rely on to function (often taking advantage of this to promote the legitimacy of their product).

Figure 1 (see next page) demonstrates how the concretization of security is bound to a cyclical process that serves to create further insecurity: Here we can see a multidimensional reflexivity bound to the performative function of 'security' that can illuminate this process. Beginning with ontological insecurities based on unknown fears, monitoring and information-gathering is used to make strangers and potential threats known. Once potential threats become known, they can be categorized into friend/enemy dichotomies, informed by political agendas, commercial interests, etc. Once enemies are constructed/fabricated, they can then be concretized as dangers through mediated events and synoptic practices; this process creates a perceived determinability (often used to legitimize security providers or agencies from which these results originate). This perception that future unknown threats can be determined perpetuates further ontological insecurities about 'not knowing' – this time about the potential for both new unknown threats *in addition to* anxiety about not being able to cope with politicized dangers (this is why I say the reflexivity is multidimensional), thus leading back to further monitoring to address these fears and create order out of chaos and so on ad infinitum.

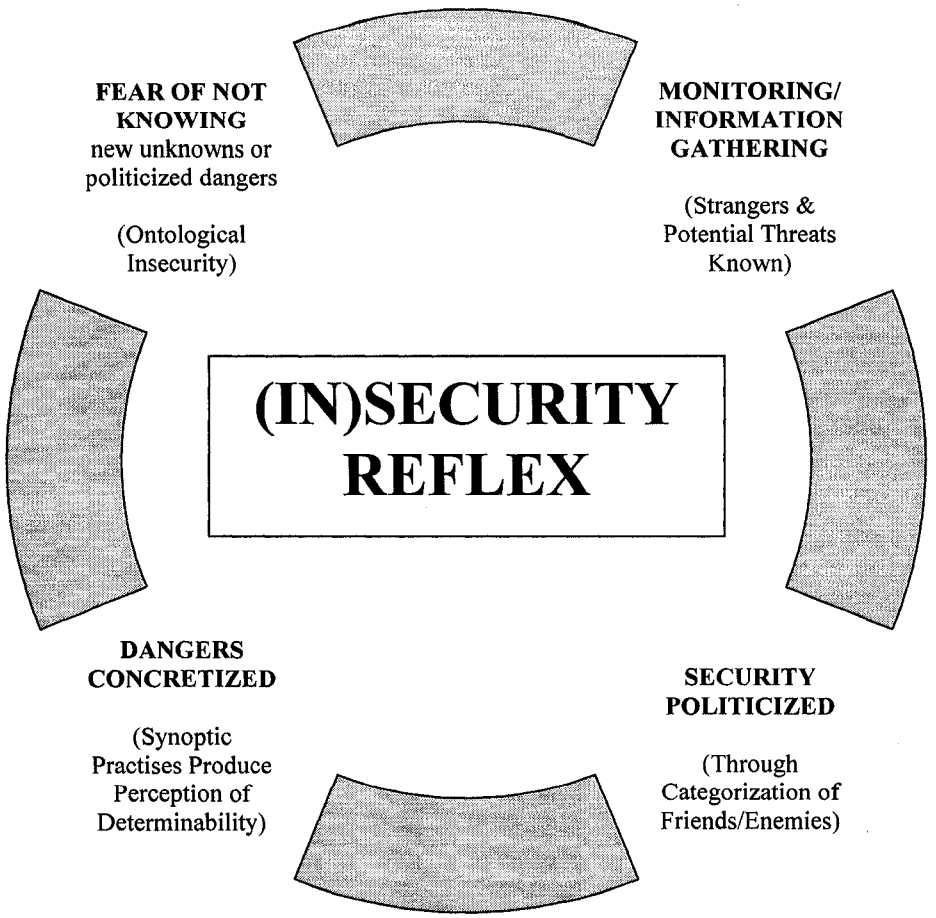

Figure 1

Ultimately then, it is argued here that more transparency is required, particularly in legislative processes that seek to address vague fears about insecurity. Inconsistencies in legislation opened a space for new enterprises to emerge to deal with perceived threats, as was the case of private security companies that worked in the spaces between police jurisdiction (though limits to the extent of their powers led to reliance on the police to sometimes take part, helping to establish informal networks for information-sharing). Expanding the powers of monitoring agencies as was seen in New Zealand should be required to have the same kinds of justification as the expansion of punitive faculties, because often the results infringe upon private citizens (as per Jones, 2000; Zedner, 2003), often in pre-emptive restrictions of access. The mentality that danger is always looming in the distance, as was seen in the case of New Zealand's Censorship Compliance Unit, sometimes leads to pre-emptive rather than preventive strategies that

hinge on particular agendas. Such was also the case with the GCSB's monitoring of foreign elements in New Zealand, where danger was presumed to abound, the only oversight being located in the ministerial realm, suspect to political influence. Many responses to perceived security threats were also seen to be only simulations of order, relying on perceived credibility as opposed to proven worth at preventing threats; this leads to further reliance on trust, especially where continuing technological advances do not allow for self-reliance in governing the limitless realm of unknown threats. It should be recognized that 'security' utterances are accompanied by ontological anxieties and have a performative power in ordering social relations, and therefore, more care must be given to limit their frequent usage.

REFERENCES

Bajc, V. 2007. "Introduction: Debating Surveillance in the Age of Security," *American Behavioral Scientist*, 50(12):1567-1591.

Bauman, Z. 2000. *Liquid Modernity*, Polity Press: Cambridge.

Beck, U., W. Bonss, and C. Lau. 2003. "The Theory of Reflexive Modernization: Problematic, Hypotheses, and Research Programme," *Theory, Culture, and Society*, 20(2): 1-33.

Brodeur, J. & B. DuPont. 2006. "Knowledge Workers or "Knowledge" Workers?" *Policing & Society*, 16: 7-26.

C.A.S.E. Collective. 2006. "Critical Approaches to Security in Europe: A Networked Manifesto," *Security Dialogue*, 37(4): 443-487.

Deleuze, G. 1992. "Postscript on the Societies of Control," *October*, 59: 3-7.

de Lint, W. (forthcoming), "Security Intelligence in New Zealand," in S. Farson, P. Gill, M. Phythian and S. Shapiro (Eds.) *PSI Handbook of Global Security and Intelligence: National Approaches*, Praeger.

de Lint, W., S. Virta, and J.E. Deukmedjian. 2007. "The Simulation of Crime Control: A Shift in Policing?" *American Behavioral Scientist*, 50(12): 1631-1647.

de Lint, W., R. Gostlow, and A. Hall. 2005. "Judgement by Deferral: The Interlocutory Injunction in Labour Disputes Involving Picketing," *Canadian Journal of Law and Society*, 20(2): 67-93.

de Lint, W. & S. Virta. 2004. "Security in ambiguity: Towards a radical security politics," *Theoretical Criminology*, 8: 465-489.

Dillon, M. 2007. "Governing through contingency: The security of biopolitical governance," *Political Geography*, 26(1):41-47.

Foucault, M. 1971. "Orders of Discourse," *Social Science Information*, 10(7): 7-30.

Foucault, M. 1991. "Governmentality," in: Burchell, G. and Miller, P. (Eds.), *The Foucault Effect: Studies in Governmentality*, University of Chicago Press, Chicago, Illinois, pp. 87-104.

Garland, D. 2002. *The Culture of Control: Crime and Social Order in Contemporary Society*, Oxford University Press: Oxford.

Giddens, A. 1990. "The Contours of High Modernity," in: *Modernity and Self-Identity*, Polity Press, London, pp. 10-34.

Grabosky, P. 2001. "Virtual Criminality: Old Wine in New Bottles?" *Social and Legal Studies*, 10(2): 243-249.

Holquist, P. 1997. "'Information is the alpha and omega of our work': Bolshevik surveillance in its pan-European context," *Journal of Modern History*, 69(3): 412-450.

Huysmans, J. 1998. "Security! What Do You Mean? From Concept to Thick Signifier," *European Journal of International Relations*, 4(2): 226-255.

Innes, M. 2001. "Control Creep," *Sociological Research Online*, 6(3): http://www.socresonline.org.uk/6/6/innes.html.

Jones, R. 2000. "Digital Rule," *Punishment and Society*, 2(1): 5-22.

Mathiesen, T. 1997. "The viewer society: Michel Foucault's 'panopticon' revisited," *Theoretical Criminology*, 1: 215-234.

Möllering, G. 2001. "The Nature of Trust: From Georg Simmel to a Theory of Expectation, Interpretation, and Suspension," *Sociology*, 35(2): 403-420.

Mouffe, C. 2005. *On the Political*, Routledge, London.

Rose, N. 1999. *Powers of Freedom: Reframing political thought*, Cambridge: UK.

Neal, A. 2006. "Foucault in Guantánamo: Towards an Archaeology of the Exception," *Security Dialogue*, 37(1): 31-46.

Schmitt, C. 1932/79. *Der Begriff des Politischen.* Berlin: Duncker and Humblot.

Spiegelman, A. 2004. *In the Shadow of No Towers*, New York: Viking.

Stehr. N. 2003. "The social and political control of knowledge in modern societies," *International Social Science Journal: UNESCO (United Nations Educational, Scientific, and Cultural Organization)*, 178: 643-655.

Tilly, C. 2004. "Trust and rule," *Theory and Society,* 33: 1-30.

Urry, J. 2002. "The Global Complexities of September 11th," *Theory, Culture, and Society*, 19: 57-69.

Walters, W. 2006. "Border/Control," *European Journal of Social Theory*, 9(2): 187-203.

Young, J. 1998. "From Inclusive to Exclusive Society: Nightmares in the European Dream," in: V. Ruggiero, N. South, and I. Taylor (Eds.) *The New European Criminology: Crime and Social Order in Europe*, Routledge, London, pp. 64-91.

Zedner, L. 2003. "Too much security?" *International Journal of the Sociology of Law*, 31: 155-184.

VITA AUCTORIS

Christian Pasiak was born in 1980 in Sault Ste Marie, Ontario. He graduated from St. Mary's College in 1999 as an Ontario Scholar. From there he went on to Lake Superior State University where he obtained a Bachelor of Science in Sociology with a Minor in Public Relations in 2003. After completing the requirements for the Master of Arts degree in Sociology at the University of Windsor in 2007, Christian will begin studies in pursuit of the degree of Doctor of Philosophy in Sociology at Carleton University.